

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
AUGUSTA DIVISION**

UNITED STATES OF AMERICA,	)	
	)	
v.	)	CASE NO. 1:17-CR-34-JRH-BKE
	)	
REALITY LEIGH WINNER,	)	
	)	
Defendant.	)	

**DEFENDANT’S MOTION AND BRIEF IN OPPOSITION TO THE
GOVERNMENT’S MOTION FOR A PROTECTIVE ORDER**

This brief is submitted in opposition to entry of the protective order as proposed by the Government unless the additions, deletions and modifications proposed herein are incorporated into the protective order. Defense Counsel seek a bright-line rule, a “rule that tends to resolve issues, especially ambiguities, simply and straightforwardly.” Black’s Law Dictionary. The order, as proposed by the Government, creates unnecessary ambiguity and imposes unnecessary impediments for the Defense.

As noted at the hearing held June 27, 2017, the Defendant moves that the following sentence be added to paragraph 4.B of the proposed protective order:

Information drawn from unclassified sources does not become classified information because similar information also happens to appear in classified documents.

Defendant further moves that the following provision be added following the first sentence of paragraph sixteen of the protective order:

Copies of newspaper articles and other publicly published documents need not be filed under seal.

Defendant further moves that Paragraph 13 of the proposed order be deleted and that the following provision be inserted as Paragraph 13:

13. The Defendant's counsel shall be given access to classified national security documents and information as required by the government's discovery obligations and in accordance with the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding described below, and any other orders issued pursuant to CIPA, and upon receipt of appropriate security clearances. Defendant Reality Leigh Winner (hereinafter "the Defendant") will also be given access to national security documents and information as required by government discovery obligations and in accordance with the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding described below, and any other orders pursuant to CIPA. Defense counsel and the Defendant will be given access to the same classified information.

Defendant further moves that the protective order provide in paragraph fifteen:

The Classified Information Security Officer shall not disclose to counsel for the government the names of experts who, with appropriate security clearances, have inspected classified information at the request of Defense counsel.

Defendant objects to the language in paragraph 19.F of the Government's proposed order that states, "including the defendant and defense witnesses," and the sentence that states, "Counsel for the government shall be given the opportunity to be heard in response to any defense request for disclosure to a person not named in this Order." These provisions should be deleted.

Defendant objects to the language in the last sentence of paragraph 19.H of the Government's proposed order that states, "that counsel does not know or have reason to believe to be classified information or derived from classified information."

Defendant moves that the language set out in bold print below be added to paragraph 22 of the Government's proposed order so that the first sentence of that paragraph states:

It shall not violate this Order for an individual subject to this Order to disclose information **in the public domain** or information that the individual did not know, and reasonably should not have known based on information provided by the

government in this case, is classified.

The Defense moves the Court to enter the protective order attached at Tab A.

ARGUMENT AND CITATION OF AUTHORITY

The issues raised by the Government's proposed protective order and the objections thereto by the Defense will be fundamental and recurring in this case. These issues should be considered in addressing the matter of the protective order.

Defendant Reality Winner is charged with espionage, conduct traditionally viewed as stealing military secrets and providing those secrets to an enemy of the United States.¹ The indictment charges a violation of 18 U.S.C. § 793(e), a statute first enacted in 1917 and entitled the Espionage Act of 1917. This statute was enacted long before there existed the system of classification of government documents under which the Government now designates matters as classified, secret and top secret. Our Government's classification system is established by executive order and not by any statute enacted by Congress.

The present language of § 793(e) was enacted in 1950 as an amendment to the Espionage Act. Section 793(e) provides:

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

¹ Black's Law Dictionary defines *espionage* as, "The activity of using spies to collect information about what another government or company is doing or plans to do."

An oft-cited and lengthy study of the history of the Espionage Act of 1917 is to be found in a 1973 Columbia Law Review article. H. Edgar and B.C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 Colum. L. Rev. 929. The authors noted:

A number of legislative proposals have been introduced since 1950 that can only reflect the assumption that the espionage statutes do not prohibit non-culpable disclosure of properly classified information. Whether the lack of coverage was seen as stemming from the problems of giving meaning to the entitlement concept is not clear. Other reasons for the proposals may have been the notion that all the espionage statutes, including 793(d) and (e), require a showing of purpose to injure the United States or advantage a foreign nation, or that proof of defense-relatedness would compromise the security interests of the classification program. Yet, if the only problem with current statutes were proof of defense-relatedness, one would expect the subsequent proposals to have been justified in terms of that legislative purpose. They have not been so justified.

Perhaps the most significant of these proposals, that of the Government Security Commission, would have made unauthorized disclosure of classified information a crime. The measure made no progress at all in Congress, and was abandoned by the Executive as politically untenable. A similar proposal had been advanced in 1946 by the Joint Congressional Committee on the Investigation of the Pearl Harbor Attack. It was severely cut back by the Judiciary Committees and wound up as the current section 798 of Title 18 which prohibits disclosure of the narrow category of classified communications intelligence information. In 1962, Senator Stennis introduced a bill to amend section 793 to make disclosures of classified information a crime, without any narrow intent requirement. The proposal was not enacted. If the classification system were thought to be protected by criminal sanctions against “willful” disclosure of defense-related information, it is remarkable that two Commissions and a Senator knowledgeable about the laws relating to national security would have seen a need for these proposals.

Id. at 1056 (emphasis added).

The authors further note:

The Executive has nowhere asserted that communication of classified information to a person not authorized by Executive regulations to receive it is a crime. The “classification stamps” are at most circuitous references to penal sanction that hardly bespeak Executive confidence that its rules and regulations give meaning to the entitlement concept. Finally, legislation has been offered from authoritative sources that proceeds on the assumption that 793(d) and (e) do not make

simple disclosure of defense information a crime. **Congress has always refused to enact such proposals to put criminal sanctions of general scope behind the classification system.**

Id. at 1057 (emphasis added).

Congress did subsequently pass a statute in 2000 that would have expressly criminalized the disclosure of classified information. H.R. Doc. No. 106-309, at 3-4 (2000). However, the bill was vetoed. *See* M.R. Papandrea, *Lapdogs, Watchdogs and Scapegoats: The Press and National Security Information*, 83 Ind. L. J. 233, 262-264 (2008). A copy of the relevant portion of the bill that was vetoed is at Tab B.

Prosecution under the Espionage Act of those who are labeled as “whistle blowers” and “leakers” is of recent origin, with most prosecutions having been brought in the last decade.

Moreover, the statutory term *national defense* refers to military action:

National defense, the Government maintains, ‘is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.’ We agree that the words ‘national defense’ in the Espionage Act carry that meaning.

. . . .

The reports [at issue], in short, are a part of this nation's plan for armed defense.

Gorin v. U.S.; 312 U.S. 19, 28-29 (1941).

An internal C.I.A analysis of this area of law that has since been declassified confirms the narrow scope of the term *national defense* secrets:

It was not until 1911, however, that Congress passed the first important statute dealing with the broad problem of espionage. In 1917 the language of the 1911 act was amended to read much as it does today. More recently congressional attention has been focused – and appropriate legislation enacted – on the problems involved in protecting atomic energy data and communications intelligence. The Internal Security Act of 1950 made it unlawful for a government employee merely to communicate classified information to a known representative of a foreign

government.

However, the espionage laws are still the basic statutory protection against unauthorized disclosure of intelligence materials and information. No legislation has yet been enacted to cover the new problems arising out of the chronic “cold war” status of international relations and the consequent need for a sophisticated, professional intelligence apparatus as an arm of the executive. The wartime concept of the military secret is inadequate to cover information about the personnel, activities, and products of such an apparatus, information whose extreme sensitivity is often not readily apparent even though its exposure may have a most damaging effect on the national security.

John D. Morrison, Jr., *The Protection of Intelligence Data*, p. 70 (copy at Tab C).

The article expresses a need for new legislative action in the form of “a criminal statute defining what is to be protected and providing punishment for exposures.” *Id.* at p. 78. As noted above, no such “new” criminal statute has as yet been enacted into law. Mr. Morrison formerly served as assistant general counsel of the C.I.A.

Russian attempts to interfere with our elections are despicable, but whether information about these Russian efforts falls within the scope of information about the secret activities of our army and navy that the Espionage Act was enacted to protect is doubtful.

A. The Protective Order Should Not Restrict Defense Counsel’s Use of Information In the Public Domain.

Dissemination of information found in “reports relating to the national defense, published by authority of Congress or the military” is not forbidden by the Espionage Act. *Gorin*, 312 U.S. at 28. *Accord, United States v. Heine*, 151 F.2d 813 (2d Cir. 1945) (L. Hand, J.) wherein the conviction of a German spy under the Espionage Act was reversed, with the Court noting:

All of this information came from sources that were lawfully accessible to anyone who was willing to take the pains to find, sift and collate it;

Id. at 815.

The Court then held:

It is not necessary for us to go so far; and in any event ‘secrets’ is an equivocal word whose definition might prove treacherous. It is enough in the case at bar to hold, as we do, that whatever it was lawful to broadcast throughout the country it was lawful to prepare and publish domestically all that Heine put in his reports.

Id. at 816.

These authorities cast doubt on the propriety of the terms of the proposed protective order that go beyond imposing restrictions on divulging what is in classified documents and information to be produced by the Government at the restricted site under the supervision of the Classified Information Security Officer.

Defense Counsel construe the protective order as proposed by the Government as imposing restrictions upon our right to cite and quote information in the public domain, such as articles in newspapers, broadcast journalism and online publications, without fear of sanctions or worse. See Paragraphs 4.B, 16 and 19; Doc. 42-1, pp. 2, 7, 11.

The order as proposed by the Government imposes upon Defense Counsel the duty to question the source of reports in the New York Times or matters discussed on Morning Joe and then to confer with the security officer before repeating or citing these facts even though the information is clearly in the public domain. The proposed “knew or have reason to know” standard is scary. What if a *fact* reported in the Washington Post can also be found within the third paragraph of a document bearing a bates stamp page number 2037, marked confidential and produced by the Government at the safe location? How would Defense Counsel be expected to assess the legitimacy of the Washington Post’s source? Would this disclosure by the Government at page 2037 meet the Government’s proposed “reason to know” standard? Would counsel for the Defense be in violation

of the Government's proposed protective order if Defense Counsel quotes the Washington Post article without having first sought permission from the security officer? Why should Defense Counsel be placed into the role of making security assessments of information in the public domain?

The dilemma that would be imposed upon Defense Counsel if the Government's proposed protective order were entered by the Court is illustrated by the January 6, 2017, article published in the Atlantic and attached at Tab D. We know not all sources reviewed by the authors. The Atlantic article does, however, contain the following statements:

These conclusions had previously been reported, based accounts anonymous intelligence officials gave to various news outlets.

Id. at p. 2.

After reviewing a classified version of the assessment made public on Friday, Trump issued a statement citing the cyber threat from "Russia, China, other countries, outside groups and people," but emphasizing that the hacking had "absolutely no effect on the outcome of the election."

Id. at p. 2.

Information on what exactly happened has been dripping out slowly, and often anonymously and unofficially, for months.

Id. at p. 4.

It wasn't until September that anonymous federal officials confirmed to *The New York Times* the intelligence community's "high confidence" of Russian government involvement in the hack, if not the subsequent leak, and leaving doubt as to whether the hacks were "routine cyberespionage" or actually intended to influence the election.

Id. at p. 4.

Then *The Washington Post* disclosed a "secret CIA assessment" – again described by anonymous officials - declaring it "quite clear" that a Trump presidency was the ultimate goal of the hacks.

Id. at p. 5.

A U.S. diplomatic cable, published in WikiLeaks, called the Baltic state an “unprecedented victim of the world’s first cyber attacks against a nation state.”

Id. at p. 6.

When they hit the NSA, hackers posted the agency’s “cyber-weapons” to file-sharing sites, according to *Esquire*.

Id. at p. 7.

Was any of this information drawn from classified sources that had not been officially declassified? One can fairly infer that some of it may have.

Defense Counsel construe the proposed provisions found in paragraphs 4.B, 16 and 19.G as setting up barriers to use of this article that would require Defense Counsel to compare facts found in the article with all classified documents produced by the Government in order to ascertain whether counsel “should . . . have known based on information provided by the government in this case” that the Atlantic article contained information drawn from classified documents. And what if, in review, counsel failed to appreciate some fact appearing in one paragraph of one page of one of perhaps hundreds of classified documents produced by the Government?

Counsel clearly have a present right to read, copy and cite this article from the Atlantic. *See, United States v. Heine, supra*. This right should not be impaired.

Defense Counsel are presently free to read, copy and cite from the public domain without seeking permission from the Government. There is no good cause for any restriction of our rights and freedom to continue to do so.

B. Defendant’s Right to Inspect Classified Documents

The Government’s proposed protective order does not allow inspection by the Defendant of

the classified documents. Doc. 42 ¶¶ 12, 13. Entry of an order with this restriction would impair Ms. Winner's Sixth Amendment right to confront the witnesses and the evidence against her and would impair her attorneys' efforts to provide effective assistance of counsel. The protective order, as written, would bar her attorneys from fully conferring with her as to relevant evidence and to learn from Ms. Winner her side of the story.

The Sixth Amendment right to counsel includes the right to confer with counsel. Restrictions imposed upon the right of a defendant to confer with counsel during trial recesses have been reversed as violations of the Sixth Amendment. *E.g.*, *Geders v. United States*, 425 U.S. 80, 88 (1976); *Hall v. Warden*, ___ Fed.App. ___, 2017 WL 1405208 * 7 (11th Cir.); *United States v. Cavallo*, 790 F.3d 1202, 1213 (11th Cir. 2015). A defendant's constitutional right to confer with counsel surely includes a right to confer about the evidence, be it favorable or not.

The court in *United States v. Fishenko*, 2014 WL 5587191 (E.D. N.Y.) addressed the issue of a defendant's constitutional right to view classified evidence. The court held:

The issue before this Court is how to ensure the constitutional rights of criminal Defendants' vis-à-vis both (1) national security concerns attendant to the classified material in this case; and (2) physical security concerns attendant to their status as pretrial detainees. The Supreme Court has held that "[t]he right of an accused in a criminal trial to due process is, in essence, the right to a fair opportunity to defend against the State's accusations." *Chambers v. Mississippi*, 410 U.S. 284, 294, 93 S.Ct. 1038, 35 L.Ed.2d 297 (1973). Founded in the Sixth Amendment's Compulsory Process and Confrontation Clauses, a criminal defendant has a right to "a meaningful opportunity to present a complete defense." *Hawkins v. Costello*, 460 F.3d 238, 243 (2d Cir.2006) (quoting *Crane v. Kentucky*, 476 U.S. 683, 690, 106 S.Ct. 2142, 90 L.Ed.2d 636 (1986)). Thus, the Defendants' constitutional rights to assist in their own defense must not be abridged.

Id. at * 1-2.

The court further held:

In this case, although certain discoverable material has been deemed classified pursuant to CIPA, the Court recognizes that the Defendants retain constitutional rights to participate in their own defense. Thus, this Court must ensure the Defendants' constitutional rights while taking into consideration the Government's legitimate concerns with respect to national security and the need for efficiency in administering this litigation.

Id. at * 2.

Attached at Tab E are the relevant parts of a protective order entered in *United States v. Jeffrey Alexander Sterling*, Doc. 38, No. 1:10-CR-485 (LMB) (E.D. Va.) by Order of Feb. 10, 2011. This order granted the defendant access to confidential information produced by the Government. The Government cites this order in its motion, although for a different proposition. Doc. 42, p. 4. This provision was adopted over the objection of the Government. *Id.* at Doc.34, pp. 9-10. Counsel for Ms. Winner drew from that order for our proposed paragraph 13.

It should be noted that Ms. Winner has had a top secret clearance for a number of years, as had Mr. Sterling. Moreover, Ms. Winner is in jail. Her telephone calls are taped, and all of her outgoing mail is being reviewed by Government agents. There is no risk to national security that could flow from her being allowed to view the evidence that may be used against her and to consult with her counsel about the evidence.

Counsel for Ms. Winner acknowledge, as did counsel for Mr. Sterling, that courts have, in extreme cases, approved of limitations being imposed upon a defendant's access to classified information. *E.g., In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 93, 127 (2d Cir. 2008); *United States v. Hausa*, ___ F.Supp.3d. ___ (E.D. N.Y. 2017), 2017 WL 1372660 * 4 (conspiracy to bomb a U.S. government facility); *United States v. Fawwaz*, 2014 WL 6997604 * 1-4

(S.D. N.Y.) (conspiracy to kill Americans with bombs and other means); *United States v. Moussaoui*, 2002 WL 1987964 (E.D. Va.) (conspiracy to commit acts of terrorism). The court in *Hausa* succinctly set forth the standard for resolution of this issue:

The Court must consider whether there is an “important need to protect a countervailing interest” that justifies the restriction on the defendant's ability to consult with his attorney and whether “the restriction is carefully tailored and limited.” *In re Terrorist Bombings*, 552 F.3d at 128–29 (quoting *United States v. Triumph Capital Grp., Inc.*, 487 F.3d 124, 129 (2d Cir. 2007).

U.S. v. Hausa, *supra* at * 6.

The decision in *Fishenko*, *supra*, provides an example of possible restraints:

Based on these conversations, the Court's inspections, the relevant law related to classified material, and consideration of the constitution rights of the Defendants to assist in their own defense, the Court has fashioned an appropriate solution. Defendants shall have unlimited access to the classified documents within the parameters of relevant security constraints. In order to view the materials, the Defendants will be produced to the inmate isolation cells of the Eastern District of New York. The isolation cells are equipped with bars rather than the mesh wires found in the attorney-client interview rooms. The Court finds that the mesh wires are not an adequate option because the mesh obstructs the Defendant's view of the documents.

Within the isolation cells, Defendants will not have direct access to the computers, per the legitimate security concerns of the U.S. Marshals. However, a paralegal or counsel with appropriate security clearance can manipulate and control the computers through a laptop. The Defendants will view the materials on a 20–inch screen placed immediately outside the isolation cell. The screen is large enough so that the Defendants can increase or decrease the text size of each document. The Defendant will have plain view of the documents through a sizable space between each bar. The Court finds that such a remedy is the proper balance of all parties' concerns, national security, and the security of staff while also protecting the Defendant's right to assist in his own defense.

Id. at * 3.

Ms. Winner's case is more analogous to the CIA agent in *Sterling* and the decisions in *Fishenki* and *United States v. I. Lewis Libby*, in which the Court was respectful of the needs of the

defendant. *United States v. Libby*, 467 F.Supp.2d 1 (D.D.C 2006); *United States v. Libby*, 2006 WL 3333059 (D.D.C.); *United States v. Libby*, 432 F.Supp.2d 81 (D.D.C. 2006).

Ms. Winner is not a terrorist. She is not a foreign national. She has long held a top secret clearance. She served six years in the United States Air Force and was honorably discharged. Her counsel have a clear need to be able to review with her the documents produced by the Government, and she has her Sixth Amendment right to confer with her counsel.

Should the Government disagree, the Government should be required to present to the Court compelling evidence that showing to Ms. Winner the classified documents that are to be produced in this case threatens the national security of the United States and that there are no restrictions other than barring access that can be imposed that would minimize or eliminate this risk.

C. The Identity of Defense Experts Who Inspect Documents Disclosed by the Government Should Not be Disclosed to the Government.

Paragraph 19.F of the Government's proposed protective order requires notice to the Government of the identity of anyone to whom Defense Counsel wishes to disclose the classified documents that the Government may produce. Such a provision is not only unnecessary, it gives unfair advantage to the Government.

It is common in cases, be they civil or criminal, for counsel to consult with learned experts to educate counsel and help counsel prepare. These consultations are with limited exceptions not discoverable.

In this case, the need to consult is great given the number of unusual and technical issues raised by this prosecution. Defense Counsel agree that any such expert must have the appropriate security clearance. However, this requirement can be enforced by the Classified Information

Security Officer without disclosure to the Government of the identify of such persons.

CONCLUSION

Bright-line rules should be adopted. The protective order should address classified documents and information produced by the Government. No restraints should be imposed upon use of documents and information in the public domain. The Defendant's Six Amendment rights should not be impaired.

Defense Counsel ask that the Court set a hearing to address these issues and that the protective order in the form attached at Tab A be adopted by the Court.

Respectfully Submitted,

BELL & BRIGHAM

s/ John C. Bell, Jr.

John C. Bell, Jr. (Bar No. 048600)

Titus T. Nichols (Bar No. 870662)

PO Box 1547

Augusta, GA 30903-1547

(706) 722-2014

John@bellbrigham.com

Titus@bellbrigham.com

COUNSEL FOR DEFENDANT

Tab A

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
AUGUSTA DIVISION**

UNITED STATES OF AMERICA,	)	
	)	
v.	)	CASE NO. 1:17-CR-34-JRH-BKE
	)	
REALITY LEIGH WINNER,	)	
	)	
Defendant.	)	

**DEFENDANT'S PROPOSED
PROTECTIVE ORDER**

This matter comes before the Court upon the Government's Motion for Protective Order to prevent the unauthorized use, disclosure or dissemination of classified national security information and documents that will be reviewed by or made available to, or are otherwise in the possession of, defense counsel in this case.

Pursuant to the authority granted under section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III ("CIPA"); the Security Procedures established pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9) (hereinafter the "Security Procedures"); the Federal Rules of Criminal Procedure 16(d) and 57; the general supervisory authority of the Court; and, in order to protect the national security, the Government's motion is GRANTED.

IT IS HEREBY ORDERED:

1. The Court finds that this case will involve classified national security information, the storage, handling and control of which, by law or regulation, require special security precautions, and access to which requires a security clearance and a need-to-know.

2. The purpose of this Protective Order ("Order") is to establish the procedures that must be followed by all defense counsel of record, their designated employees, all other counsel involved in this case, translators and investigators for the defense and all other individuals who receive access to classified information or documents in connection with this case.

3. The procedures set forth in this Order shall apply to all pre-trial, trial, post-trial, and appellate aspects of this case; and may be modified from time to time by further order of the Court acting under this Court's inherent supervisory authority to ensure a fair and expeditious trial.

Definitions

4. As used herein, the terms classified national security information and documents," "classified information," "classified documents," and "classified material" refer to:

- A. Any classified document or information that has been classified by any Executive Branch agency in the interest of national security or pursuant to Executive Order 13526 or its predecessor orders as "CONFIDENTIAL," or "SECRET," or "TOP SECRET," or "SENSITIVE COMPARTMENTED INFORMATION ("SCI")"; or any information contained in such documents;
- B. Any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party, which has been derived from a United States Government classified document, information, or material, regardless of whether such document, information, or material has itself subsequently been classified by the Government pursuant to Executive Order 13526 or its predecessor orders as "CONFIDENTIAL" or "SECRET," or "TOP SECRET," or "SCI;" Information drawn from unclassified sources does not become classified information

because similar information also happens to appear in classified documents.

- C. Verbal classified information known to the defense counsel;
- D. Any document or information, including verbal information, which the defense counsel have been notified orally or in writing contains classified information;
- E. Any information, regardless of place or origin and including "foreign government information" as that term is defined in Executive Order 13526, that could reasonably be believed to contain classified information; and
- F. Any information obtained from an agency that is a member of the United States "Intelligence Community" (as defined in section 3(4) of the National Security Act of 1947, codified at 50 U.S.C. § 401 a(4)), that could reasonably be believed to contain classified information or that refers to national security or intelligence matters.

5. The words "documents," "information," and "material" shall include but are not limited to all written or printed matter of any kind, formal or informal, including originals, conforming copies and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), and further include but are not limited to:

- A. Papers, correspondence, memoranda, notes, letters, reports, summaries, photographs, maps, charts and graphs, interoffice and intra-office communications, notations of any sort concerning conversations, meetings or other communications, bulletins, teletypes, telegrams and telefacsimiles, invoices, worksheets and drafts, alterations, modifications, changes and amendments of any kind to the foregoing;

- B. Graphic or oral records or representations of any kind, including but not limited to photographs, charts graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;
 - C. Electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and
 - D. Information acquired orally or verbally.
6. "Access to classified information" means having access to, reviewing, reading, learning or otherwise coming to know in any manner any classified information.
7. "Secure Area" shall mean a sensitive compartmented facility or other appropriate facility approved by a Classified Information Security Officer for storage, handling, and control of classified information.
8. All classified documents or material and the information contained therein shall remain classified unless the documents or material bear a clear indication that they have been declassified by the agency or department that is the originating agency (hereinafter the "Originating Agency") of the document, material, or information contained therein.
9. Any classified information provided to the Defense by the Government is to be used solely by the Defense and for the purpose of preparing the defense. The Defense may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.
10. Classified Information Security Officer. In accordance with the provisions of CIPA and the Security Procedures, the Court designates Carli V. Rodriguez-Feo as Classified Information

Security Officer for this case, and Debra M. Guerrero-Randall, Daniel O. Hartenstine, Joan B. Kennedy, Shawn P. Mahoney, Maura L Peterson, Winfield S. "Scooter" Slade, and Harry Rucker III, as Alternate Classified Information Officers for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information to be made available in connection with this case. Defense counsel shall seek guidance from the Classified Information Security Officer with regard to appropriate storage, handling, transmittal, and use of classified information.

11. Government Attorneys. The Court has been advised that the Government attorneys working on this case, Assistant United States Attorney Jennifer Solari and U.S. Department of Justice Attorneys Julie Edelstein and David Aaron, and their respective supervisors (collectively referred to hereinafter as the "Government Attorneys"), have the requisite security clearances to have access to the classified information that relates to this case.

12. Protection of Classified Information. The Court finds that, in order to protect the classified information involved in this case, only Government Attorneys, appropriately cleared Department of Justice employees, personnel of the Originating Agency, defense counsel, employees of defense counsel, translators, and investigators employed or hired by defense counsel, shall have access to the classified information in this case.

A. Defense counsel, employees of defense counsel or defense translators and investigators may obtain access to classified documents or information only if such person has:

- 1) Received permission of the Court, either through this Order (for those named in paragraph 13 below) or by a separate Court order upon showing of a

need-to-know;

- 2) Received the necessary security clearance at the appropriate level of classification, through or confirmed by the Classified Information Security Officer; and
- 3) Signed the Memorandum of Understanding in the form attached hereto, agreeing to comply with the terms of this Order.

B. Defense counsel shall file originals of the executed Memoranda of Understanding with the Court under seal and serve copies of such document upon the Classified Information Security Officer and the Government.

C. The substitution, departure and removal for any reason from this case of counsel for the defendant, or anyone associated with the defense as an employee or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order; and

13. Defense Counsel. The Defendant's counsel shall be given access to classified national security documents and information as required by the government's discovery obligations and in accordance with the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding described below, and any other orders issued pursuant to CIPA, and upon receipt of appropriate security clearances. Defendant Reality Leigh Winner (hereinafter "the Defendant") will also be given access to national security documents and information as required by government discovery obligations and in accordance with the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding described below, and any other orders pursuant to CIPA. Defense counsel and the Defendant will be given access to the same classified

information.

14. Unless they already hold an appropriate security clearance and are approved for access to classified information in this case, the Defense, including all persons whose assistance the Defense reasonably requires, shall complete and submit to the Classified Information Security Officer a Standard Form 86 ("Security Investigation Data for Sensitive Position"), attached releases, and "major case" fingerprints in order to obtain security clearances necessary for access to classified information that may be involved in this case. The Classified Information Security Officer shall provide access to the necessary forms. The Classified Information Security Officer shall take all reasonable steps to process all security clearance applications.

15. Secure Area of Review. The Classified Information Security Officer shall arrange for an appropriately approved Secure Area for use by the Defense. The Classified Information Security Officer shall establish procedures to assure that the Secure Area is accessible to the Defense during normal business hours, after hours, and on weekends, in consultation with the United States Marshals Service. The Secure Area shall contain a separate working area for the Defense, and will be outfitted with any secure office equipment requested by the Defense that is reasonable and necessary to the preparation of the defense in this case. The Classified Information Security Officer, in consultation with defense counsel, shall establish procedures to assure that the Secure Area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No documents or other material containing classified information may be removed from the Secure Area unless authorized by the Classified Information Security Officer. The Classified Information Security Officer shall not reveal to the Government the content of any conversations he or she may hear among the Defense, nor reveal the nature of documents being reviewed by them, nor

the work generated by them. In addition, the presence of the Classified Information Security Officer shall not operate to waive, limit, or otherwise render inapplicable, the attorney-client privilege. The Classified Information Security Officer shall not disclose to counsel for the government the names of experts who, with appropriate security clearances, have inspected classified information at the request of Defense counsel.

16. Filings with the Court. Until further order of this Court, any motion, memorandum, or other document filed by the Defense that defense counsel knows, or has reason to believe, contains classified information in whole or in part, or any document the proper classification of which defense counsel is unsure, shall be filed under seal with the Court through the Classified Information Security Officer or an appropriately cleared designee of his choosing. Copies of newspaper articles and other publicly published documents need not be filed under seal. Pleadings filed under seal with the Classified Information Security Officer shall be marked "Filed In Camera and Under Seal with the Classified Information Security Officer and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the Classified Information Security Officer or a designee, which should occur no later than 4.00 pm, shall be considered as the date and time of court filing. At the time of making a physical submission to the Classified Information Security Officer or a designee, counsel shall file on the public record in the CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title in the filing. The Classified Information Security Officer shall make arrangements for prompt delivery under seal to the Court and counsel for the Government any document to be filed by the Defense that contains classified information. The Classified Information Security Officer shall

promptly examine the document and, in consultation with representatives of the appropriate Government agencies, determine whether the document contains classified information. If the Classified Information Security Officer determines that the document contains classified information, he or she shall ensure that the classified portions of the document, and only those portions, are marked with the appropriate classification marking and that the document remains under seal. All portions of any document filed by the Defense that do not contain classified information shall immediately be unsealed by the Classified Information Security Officer and placed in the public record.

17. Any document filed by the Government containing classified information shall be filed under seal with the Court through the Classified Information Security Officer or an appropriately cleared designee of his choosing. Pleadings filed under seal with the Classified Information Security Officer or a designee shall be marked "Filed In Camera and Under Seal with the Court Information Security Officer" and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the Classified Information Security Officer or a designee, which should occur no later than 4 00pm, shall be considered the date and time of filing. The Classified Information Security Officer shall make arrangements for prompt delivery under seal to the Court and defense counsel (unless ex parte) any document to be filed by the Government that contains classified information. At the time of making a physical submission to the Classified Information Security Officer or a designee, counsel shall file on the public record in the CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title in the filing.

18. Sealing of Records. The Classified Information Security Officer shall maintain a separate sealed record for those pleadings containing classified materials, and retain such record for purposes of later proceedings or appeal.

19. Access to Classified Information. The Defense shall have access to classified information only as follows:

- A. All classified information produced by the Government to the Defense, in discovery or otherwise, and all classified information possessed, created or maintained by the Defense, shall be stored, maintained and used only in the Secure Area established by the Court Information Security Officer;
- B. The Defense shall have free access to the classified information made available to them in the Secure Area, and shall be allowed to take notes and prepare documents with respect to those materials. However, the Defense shall not, except under separate Court order, disclose the classified information, either directly, indirectly, or in any other manner which would disclose the existence of such, to pursue leads or in the defense of the defendant;
- C. The Defense shall not copy or reproduce any classified information in any form, except with the approval of the Classified Information Security Officer, or in accordance with the procedures established by the Classified Information Security Officer for the operation of the Secure Area;
- D. All documents prepared by the Defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information, shall be transcribed, recorded, typed, duplicated, copied, or otherwise

prepared only by persons who have received an appropriate approval for access to classified information, and in the Secure Area on equipment approved for the processing of classified information, and in accordance with the procedures established by the Court Information Security Officer. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, etc.) containing classified information shall be maintained in the Secure Area, unless and until the Classified Information Security Officer determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the Government;

- E. The Defense shall discuss classified information only within the Secure Area or in another area authorized by the Classified Information Security Officer, and shall not discuss or attempt to discuss classified information over any standard commercial telephone instrument or office intercommunication system; and
- F. The Defense shall not disclose, without prior approval of the Court, any classified information to any person not authorized pursuant to this Order, except to the Court, court personnel, and the Government Attorneys who have been identified by the Classified Information Security Officer as having the appropriate clearances and the need-to-know that information. Any person approved by the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to the Court the Memorandum of Understanding appended to this Order, and to comply with all terms and conditions of this Order. If preparation of the Defense requires that classified information be disclosed to persons not named in this

Order, then, upon approval by the Court, the Classified Information Security Officer shall promptly seek to obtain security clearances for them at the request of defense counsel.

- G. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who by virtue of this Order or any other court order are granted access to the classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the Defense to have such information confirmed or denied at trial or in any public proceeding in this case, the Defense must comply with the notification requirements of section 5 of CIPA and all the provisions of this Order.
- H. In the event that classified information enters the public domain, the Defense is precluded from making private or public statements where the statements would reveal personal knowledge from non-public sources regarding the classified status of the information, or would disclose that the Defense had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. The Defense is not precluded from citing or repeating information in the public domain.

20. Procedures for the use or disclosure of classified information by the Defense shall be those provided in sections 5 and 6 and 8 of CIPA. To facilitate the Defense's filing of notices required under section 5 of CIPA, the Classified Information Security Officer shall make

arrangements with the appropriate agencies for a determination of the classification level, if any, of materials or information, either within the possession of the Defense or about which the Defense has knowledge and which the Defense intends to use in any way at any pre-trial proceeding, deposition or at trial. Nothing submitted by the Defense to the Classified Information Security Officer pursuant to this paragraph shall be made available to counsel for the Government unless so ordered by the Court, or so designated by the Defense. Any and all items that are classified shall be listed in the defendant's CIPA section 5 notice. To the extent that any classified information is the basis of any motion filed by the Defense, such motion shall be preceded by a CIPA section 5 notice.

21. Violations of this Order. Unauthorized use or disclosure of classified information may constitute violations of United States criminal laws. In addition, violation of the terms of this Order shall be immediately brought to the attention of the Court, and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may result in the termination of a person's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized use, disclosure, retention or negligent handling of classified information could cause serious damage, and in some cases exceptionally grave damage, to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. This Order is to ensure that those authorized by the Order to receive classified information will never divulge the classified information disclosed to them to anyone who is not authorized to receive it, or otherwise use the classified information, without prior written authorization from the Originating Agency and in conformity with this Order.

22. It shall not violate this Order for an individual subject to this Order to disclose information in the public domain or information that the individual did not know, and reasonably should not have known based on information provided by the government in this case, is classified. Any individual subject to this Order who intends to disclose information and is not certain whether that information is classified should consult with the CISO.

23. All classified information to which the Defense has access in this case is now and will remain the property of the United States. The defense counsel, defense counsel employees, defense translators, investigators and anyone else who receives classified information pursuant to this Order shall return all such classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information, to the Classified Information Security Officer upon request. The notes, summaries and other documents prepared by the Defense that do or may contain classified information shall remain at all times in the custody of the Classified Information Security Officer or the duration of this case. At the conclusion of all proceedings, including any final appeals, all such notes, summaries and other documents are to be destroyed by the Classified Information Security Officer in the presence of defense counsel if so desired.

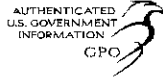
24. Nothing in this Order shall preclude the Government from seeking a further protective order pursuant to CIPA and/or Rule 16(d) of the Federal Rules of Criminal Procedure as to particular items of discovery material.

25. A copy of this Order shall be issued forthwith to counsel for the defendant, who shall be responsible for advising the defendant and defense counsel employees, of the contents of this Order.

SO ORDERED this ____ day of _____, 2017.

HON. BRIAN K. EPPS
UNITED STATES MAGISTRATE JUDGE

Tab B



In the Senate of the United States,

October 2 (legislative day, September 22), 2000.

Resolved, That the bill from the House of Representatives (H.R. 4392) entitled “An Act to authorize appropriations for fiscal year 2001 for intelligence and intelligence-related activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other purposes.”, do pass with the following

AMENDMENT:

Strike out all after the enacting clause and insert:

1 ***SECTION 1. SHORT TITLE; TABLE OF CONTENTS.***

2 (a) *SHORT TITLE.*—*This Act may be cited as the “In-*
3 *telligence Authorization Act for Fiscal Year 2001”.*

- 1 (b) *TABLE OF CONTENTS.*—*The table of contents for*
 2 *this Act is as follows:*

Sec. 1. Short title; table of contents.

TITLE I—INTELLIGENCE ACTIVITIES

- Sec. 101. Authorization of appropriations.*
Sec. 102. Classified schedule of authorizations.
Sec. 103. Personnel ceiling adjustments.
Sec. 104. Community Management Account.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

- Sec. 201. Authorization of appropriations.*

TITLE III—GENERAL PROVISIONS

- Sec. 301. Increase in employee compensation and benefits authorized by law.*
Sec. 302. Restriction on conduct of intelligence activities.
Sec. 303. Prohibition on unauthorized disclosure of classified information.
Sec. 304. POW/MIA analytic capability within the intelligence community.
*Sec. 305. Applicability to lawful United States intelligence activities of Federal
laws implementing international treaties and agreements.*
*Sec. 306. Limitation on handling, retention, and storage of certain classified ma-
terials by the Department of State.*
*Sec. 307. Clarification of standing of United States citizens to challenge certain
blocking of assets.*
*Sec. 308. Availability of certain funds for administrative costs of Counterdrug In-
telligence Executive Secretariat.*
Sec. 309. Designation of Daniel Patrick Moynihan Place.

TITLE IV—CENTRAL INTELLIGENCE AGENCY

- Sec. 401. Expansion of Inspector General actions requiring a report to Congress.*
Sec. 402. Subpoena authority of the Inspector General.
Sec. 403. Improvement and extension of central services program.
Sec. 404. Details of employees to the National Reconnaissance Office.
Sec. 405. Transfers of funds to other agencies for acquisition of land.
*Sec. 406. Eligibility of additional employees for reimbursement for professional
liability insurance.*

TITLE V—DEPARTMENT OF DEFENSE INTELLIGENCE ACTIVITIES

- Sec. 501. Two-year extension of authority to engage in commercial activities as
security for intelligence collection activities.*
*Sec. 502. Role of Director of Central Intelligence in experimental personnel pro-
gram for certain scientific and technical personnel.*
*Sec. 503. Prohibition on transfer of imagery analysts from General Defense Intel-
ligence Program to National Imagery and Mapping Agency Pro-
gram.*
*Sec. 504. Prohibition on transfer of collection management personnel from Gen-
eral Defense Intelligence Program to Community Management
Account.*
Sec. 505. Authorized personnel ceiling for General Defense Intelligence Program.

Sec. 506. Measurement and signature intelligence.

TITLE VI—COUNTERINTELLIGENCE MATTERS

Sec. 601. Short title.

Sec. 602. Orders for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978.

Sec. 603. Orders for physical searches under the Foreign Intelligence Surveillance Act of 1978.

Sec. 604. Disclosure of information acquired under the Foreign Intelligence Surveillance Act of 1978 for law enforcement purposes.

Sec. 605. Coordination of counterintelligence with the Federal Bureau of Investigation.

Sec. 606. Enhancing protection of national security at the Department of Justice.

Sec. 607. Coordination requirements relating to the prosecution of cases involving classified information.

Sec. 608. Severability.

TITLE VII—DISCLOSURE OF INFORMATION ON JAPANESE IMPERIAL ARMY

Sec. 701. Short title.

Sec. 702. Establishment of Japanese Imperial Army Records Interagency Working Group.

Sec. 703. Requirement of disclosure of records.

Sec. 704. Expedited processing of FOIA requests for Japanese Imperial Army records.

Sec. 705. Effective date.

TITLE VIII—DECLASSIFICATION OF INFORMATION

Sec. 801. Short title.

Sec. 802. Findings.

Sec. 803. Public Interest Declassification Board.

Sec. 804. Identification, collection, and review for declassification of information of archival value or extraordinary public interest.

Sec. 805. Protection of national security information and other information.

Sec. 806. Standards and procedures.

Sec. 807. Judicial review.

Sec. 808. Funding.

Sec. 809. Definitions.

Sec. 810. Sunset.

1 TITLE I—INTELLIGENCE 2 ACTIVITIES

3 SEC. 101. AUTHORIZATION OF APPROPRIATIONS.

4 (a) AUTHORIZATION OF APPROPRIATIONS FOR FISCAL
5 YEAR 2001.—*Funds are hereby authorized to be appro-*
6 priated for fiscal year 2001 for the conduct of the intel-

1 *as may be necessary for increases in such compensation or*
2 *benefits authorized by law.*

3 **SEC. 302. RESTRICTION ON CONDUCT OF INTELLIGENCE**
4 **ACTIVITIES.**

5 *The authorization of appropriations by this Act shall*
6 *not be deemed to constitute authority for the conduct of any*
7 *intelligence activity which is not otherwise authorized by*
8 *the Constitution or the laws of the United States.*

9 **SEC. 303. PROHIBITION ON UNAUTHORIZED DISCLOSURE**
10 **OF CLASSIFIED INFORMATION.**

11 *(a) IN GENERAL.—Chapter 37 of title 18, United*
12 *States Code, is amended—*

13 *(1) by redesignating section 798A as section*
14 *798B; and*

15 *(2) by inserting after section 798 the following*
16 *new section 798A:*

17 **“§798A. Unauthorized disclosure of classified infor-**
18 **mation**

19 *“(a) PROHIBITION.—Whoever, being an officer or em-*
20 *ployee of the United States, a former or retired officer or*
21 *employee of the United States, any other person with au-*
22 *thorized access to classified information, or any other per-*
23 *son formerly with authorized access to classified informa-*
24 *tion, knowingly and willfully discloses, or attempts to dis-*
25 *close, any classified information acquired as a result of such*

1 *person's authorized access to classified information to a per-*
2 *son (other than an officer or employee of the United States)*
3 *who is not authorized access to such classified information,*
4 *knowing that the person is not authorized access to such*
5 *classified information, shall be fined under this title, im-*
6 *prisoned not more than 3 years, or both.*

7 “(b) *CONSTRUCTION OF PROHIBITION.*—*Nothing in*
8 *this section shall be construed to establish criminal liability*
9 *for disclosure of classified information in accordance with*
10 *applicable law to the following:*

11 “(1) *Any justice or judge of a court of the United*
12 *States established pursuant to article III of the Con-*
13 *stitution of the United States.*

14 “(2) *The Senate or House of Representatives, or*
15 *any committee or subcommittee thereof, or joint com-*
16 *mittee thereof, or any member of Congress.*

17 “(3) *A person or persons acting on behalf of a*
18 *foreign power (including an international organiza-*
19 *tion) if the disclosure—*

20 “(A) *is made by an officer or employee of*
21 *the United States who has been authorized to*
22 *make the disclosure; and*

23 “(B) *is within the scope of such officer's or*
24 *employee's duties.*

1 “(4) Any other person authorized to receive the
2 classified information.

3 “(c) DEFINITIONS.—In this section:

4 “(1) The term ‘authorized’, in the case of access
5 to classified information, means having authority or
6 permission to have access to the classified information
7 pursuant to the provisions of a statute, Executive
8 Order, regulation, or directive of the head of any de-
9 partment or agency who is empowered to classify in-
10 formation, an order of any United States court, or a
11 provision of any Resolution of the Senate or Rule of
12 the House of Representatives which governs release of
13 classified information by such House of Congress.

14 “(2) The term ‘classified information’ means in-
15 formation or material properly classified and clearly
16 marked or represented, or that the person knows or
17 has reason to believe has been properly classified by
18 appropriate authorities, pursuant to the provisions of
19 a statute or Executive Order, as requiring protection
20 against unauthorized disclosure for reasons of na-
21 tional security.

22 “(3) The term ‘officer or employee of the United
23 States’ means the following:

24 “(A) An officer or employee (as those terms
25 are defined in sections 2104 and 2105 of title 5).

1 “(B) *An officer or enlisted member of the*
 2 *Armed Forces (as those terms are defined in sec-*
 3 *tion 101(b) of title 10).’.*”

4 (b) *CLERICAL AMENDMENT.—The table of sections at*
 5 *the beginning of that chapter is amended by striking the*
 6 *item relating to section 798A and inserting the following*
 7 *new items:*

 “798A. *Unauthorized disclosure of classified information.*

 “798B. *Temporary extension of section 794.’.*”

8 **SEC. 304. POW/MIA ANALYTIC CAPABILITY WITHIN THE IN-**
 9 **TELLIGENCE COMMUNITY.**

10 *Title I of the National Security Act of 1947 (50 U.S.C.*
 11 *402 et seq.) is amended by adding at the end the following:*

12 “**POW/MIA ANALYTIC CAPABILITY**

13 “**SEC. 115. (a) REQUIREMENT.—**(1) *The Director of*
 14 *Central Intelligence shall, in consultation with the Sec-*
 15 *retary of Defense, establish and maintain in the intelligence*
 16 *community an analytic capability with responsibility for*
 17 *intelligence in support of the activities of the United States*
 18 *relating to unaccounted for United States personnel.*

19 “(2) *The analytic capability maintained under para-*
 20 *graph (1) shall be known as the ‘POW/MIA analytic capa-*
 21 *bility of the intelligence community’.*

22 “(b) **SCOPE OF RESPONSIBILITY.—***The responsibilities*
 23 *of the analytic capability maintained under subsection (a)*
 24 *shall—*

Tab C

4-39-4

OFFICIAL USE ONLY

*Historical review of the problem
and some remedial proposals.*

THE PROTECTION OF INTELLIGENCE DATA

John D. Morrison, Jr.

The unauthorized exposure of classified information is a chronic problem for governments and intelligence agencies. Defense against the conscious agent of a foreign power is different from, and in some ways less difficult than, deterring revelations due to carelessness, malice, or greed on the part of government employees. The problem is particularly acute in a democratic society whose laws and courts must provide broad protection to criminal defendants. The deterrence provided by the espionage laws and related statutes is weakened by the difficulty of prosecution under them. This is especially true in cases involving disaffected or careless employees of intelligence agencies; the defenses usually include strong equitable pleas which may excite a sympathetic public response.

No legislation or administrative procedure can offer perfect protection. It is submitted, however, that both our laws and our administrative procedures could be improved so as to provide more effective deterrence. Some particular avenues that might be taken will emerge from the following discussion.

The Espionage Laws: An Incomplete Structure

A review of American legislation in the field of criminal espionage shows that historically there has been limited legislative effort directed to the protection of intelligence data. As a result there is a startling lack of protection for a governmental function of growing importance and sensitivity. Perhaps the need for laws protecting intelligence data has reached significant proportions only in the relatively recent past.

The changes, technological and other, in the manner in which nations deal with each other have caused some improvements in legislation dealing with the protection of state secrets. Diplomatic communications have traditionally been protected. As early as 1807, the Supreme Court suggested that the legislature recognize and provide against crimes affecting the national security which have

OFFICIAL USE ONLY

69

OFFICIAL USE ONLY

Legal Protection

not ripened into treason."¹ It was not until 1911, however, that Congress passed the first important statute dealing with the broad problem of espionage. In 1917 the language of the 1911 act was amended to read much as it does today. More recently congressional attention has been focused—and appropriate legislation enacted—on the problems involved in protecting atomic energy data² and communications intelligence.³ The Internal Security Act of 1950⁴ made it unlawful for a government employee merely to communicate classified information to a known representative of a foreign government.⁵

However, the espionage laws⁶ are still the basic statutory protection against unauthorized disclosure of intelligence materials and information. No legislation has yet been enacted to cover the new problems arising out of the chronic "cold war" status of international relations and the consequent need for a sophisticated, professional intelligence apparatus as an arm of the executive. The wartime concept of the military secret is inadequate to cover information about the personnel, activities, and products of such an apparatus, information whose extreme sensitivity is often not readily apparent even though its exposure may have a most damaging effect on the national security.

These shortcomings point to the need for new legislation establishing a category "Intelligence Data" and providing that anything so designated by an authorized official shall be judicially recognized as such solely on the basis of that designation. This would solve a vexatious and recurring problem for which there is no known cure in existing laws. That problem is the immunity enjoyed by an exposé of sensitive information when the information itself cannot for practical reasons be brought into the open for the purpose of prosecution.

The Official Secrets Acts

It has often been suggested that, if legislation is needed in this area, the British Official Secrets Acts with their broader protection offer a good example to be followed. It is not commonly understood

¹ Ex parte Bollman and Ex parte Swartwout, 4 Cranch 75, 127, 2 L. Ed. 554, 571 (1807).

² 42 U.S.C. §2271 et seq.

³ 18 U.S.C. §793.

⁴ 50 U.S.C. §783(b).

⁵ See *Scarbeck v. U.S.*, 317 F. 2d 546, cert. denied, 83 S. Ct. 1897 (1963).

⁶ 18 U.S.C. §§791-798.

Legal Protection

OFFICIAL USE ONLY

that the British acts are based on a different legal theory from that underlying our espionage acts. Under our system the information divulged must be shown to be related to national defense and security either by its very nature or as coming within statutory definitions such as those for communications intelligence and atomic energy data. The British acts are based on the theory of privilege, according to which all official information, whether or not related to the national defense and security, is the property of the crown. It is therefore privileged, and those who receive it officially may not divulge it without the crown's authority.

In a British prosecution for unauthorized disclosure several consequences flow from the privilege theory. Portions of the trial can be held *in camera* if the court agrees. Under our constitution, while certain procedural aspects can be considered *in camera*, no part of the actual trial could be heard privately. In Britain certain presumptions may apply. For instance, if the defendant is known to have possession of privileged information and to have been in the company of a known foreign espionage agent, there is a presumption that he passed the information. The presumption is rebuttable; but our Supreme Court opinions indicate that such a presumption would not be permissible here. Most important, in the English system it is not necessary to prove that any item of information relates to the national defense and security.

A good example is the so-called Isis case in which two Oxford students published in their college magazine, *Isis*, the story of their experiences in the Navy, including technical intelligence operations in the Baltic. The prosecution merely testified that the article contained information which they had acquired in their official service and was, therefore, privileged. After the verdict of guilty, the prosecution approached the court alone, without presence of defendants or defense counsel, and briefed the court, solely for purposes of sentencing, on the significance of each item of information to the government. Such a briefing, we believe, would be held error under our system.⁷

In another case, that of an RAF officer named Wraight who defected to Russia and then returned, a government witness who had inter-

⁷ *Jencks v. U.S.*, 353 U.S. 657, 668 (1957). But see post *Jencks* Statute 18 U.S.C. §3500(c) permitting *in camera* examination for relevancy and editing of pre-trial reports of government witnesses.

OFFICIAL USE ONLY

OFFICIAL USE ONLY

Legal Protection

viewed the defendant for the security services was allowed to testify without publicly identifying himself. His name was handed in writing to the court. Possibly this could be done here if the defense agreed to it, but it seems clear it could not be done over the defense's objection.

In short, the Official Secrets Acts would seem to be in important respects unconstitutional in this country and therefore cannot be relied on as examples of means by which we could protect intelligence data. In addition, despite the technical advantages which the British laws provide for the prosecution, experience has shown that these do not by any means give complete protection; they are only to some degree more effective than our system.

Intelligence Sources and Methods

The statutory authorities and responsibilities of the Director of Central Intelligence include the responsibility for "protecting intelligence sources and methods from unauthorized disclosure."⁸ The Congress's use of the term "intelligence sources and methods" indicates its recognition of the existence of a special kind of data encompassing a great deal more than what is usually termed "classified intelligence information." The espionage laws and the statutes designed to protect communications and atomic secrets, though they specify in detail the kinds of information they seek to protect, nevertheless do not cover everything that might be defined as intelligence data whose exposure could be detrimental to the national interests. For example, knowing the identities of U.S. covert intelligence officers or the fact that U.S. intelligence is making a study of certain published unclassified materials might be of great value to a foreign intelligence agency, but there is some question whether such information would be considered by a court to be included among the things protected by existing statutes.

The Congress has also recognized the need for protecting intelligence sources and methods by enacting for CIA a number of special authorities and exemptions from legal requirements otherwise in general force throughout the government. The Agency is exempted from the "provisions of any . . . law which require the publication

⁸ National Security Act of 1947, §102(d), 61 Stat. 495 50 U.S.C. §403.

Legal Protection**OFFICIAL USE ONLY**

or disclosure of the organization, functions, names, official titles, salaries, or numbers of personnel employed by the Agency."⁹ Similarly, the Agency is authorized to expend the funds made available to it for objects of a confidential, extraordinary, or emergency nature, such expenditures to be accounted for solely on the certificate of the Director. It is exempted from statutory requirements regarding exchanges of funds and the performance rating of employees and from laws and executive orders governing appeals from adverse personnel actions.

Thus Congress has charged the Director of Central Intelligence with protecting intelligence sources and methods from unauthorized disclosure, has recognized that the term "intelligence sources and methods" encompasses an area not entirely covered in other statutes, and has affirmed the need for such protection by providing statutory authority for that purpose. The void in the statutory structure protecting intelligence sources and methods is the absence of sanctions against unauthorized disclosure which can be invoked without disclosing the very sources and methods whose protection is sought.

The Judicial View of Intelligence

The courts have long recognized that the secret intelligence activities of the executive branch, though indispensable to the government, are by their nature matters whose disclosure would be injurious to the public. In the *Totten* case¹⁰ compensation was sought under a secret contract with President Lincoln for espionage activities behind Confederate lines. The opinion of the Supreme Court stated:

If upon contracts of such a nature an action against the government could be maintained in the Court of Claims, whenever an agent should deem himself entitled to greater or different compensation than that awarded to him, the whole service in any case, and the manner of its discharge, with the details of the dealings with individuals and officers, might be exposed, to the serious detriment of the public. A secret service, with liability to publicity in this way would be impossible; and, as such services are sometimes indispensable to the Government, its agents in those services must look for their compensation to the contingent fund of the department employing them, and to such allowance from it as those who dispense that fund may award. The secrecy which such contracts impose precludes any action for their enforce-

⁹ Central Intelligence Agency Act of 1949, as amended, §6, 63 Stat. 208, 50 U.S.C. §403g.

¹⁰ *Totten v. U.S.*, 92 U.S. 105 (1876).

OFFICIAL USE ONLY**73**

OFFICIAL USE ONLY

Legal Protection

ment. The publicity produced by an action would itself be a breach of a contract of that kind, and thus defeat a recovery.

It may be stated as a general principle, that public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not let the confidence be violated. On this principle, suits cannot be maintained which would require a disclosure of the confidences of the confessional, or those between husband or wife, or of communications by a client to his counsel for professional advice, or of a patient to his physician for a similar purpose. *Much greater reason exists for the application of the principle to cases of contract for secret services with the Government, as the existence of a contract of that kind is itself a fact not to be disclosed.* [Emphasis supplied.]

The Totten case marks the beginning of the juridical idea—and judicial cognizance of it—that there is a kind of relationship to the state which is confidential, beyond judicial inquiry, and involving a trust of such nature that the courts cannot aid a breach of it, even in their solemn duty of administering justice.¹¹ A secret agent is almost impotent in his own cause; he literally cannot maintain an action in the courts where his secret activities are germane to the case.¹²

Judicial Access to Sensitive Data

Present espionage laws dealing with unlawful transmission or obtaining of information related to the national defense¹³ have been interpreted as requiring proof of certain questions of fact; evidence on these questions must be submitted to the jury for consideration of its weight and sufficiency. For instance, the information betrayed must in fact be related to the national defense and must not have been generally available.¹⁴ The courts have held that a jury cannot find on these facts unless it has access to the information allegedly related to the national defense and hears testimony regarding its use, importance, exclusiveness, and value to a foreign government or

¹¹ See *Firth Sterling Steel Co. v. Bethlehem Steel Co.*, 199 Fed. 353 (1912), in which the court struck documents from the record on the ground that it was against public policy to disclose military secrets. See cases cited in note 18.

¹² *De Arnaud v. U.S.*, 29 Ct. 555, 151 U.S. 483 (1894); *Allen v. U.S.*, 27 Ct. Cl. 89 (1892); *Tucker v. U.S.*, 118 F. Supp. 371 (1954).

¹³ 18 U.S.C. §§793, 794, and 798.

¹⁴ *U.S. v. Heins*, 151 F.2d 813, 818 (1945), citing *Cortin v. U.S.*, 312 U.S. 19, 28, 61 S.Ct. 429, 85 L.Ed. 488 (1941).

Legal Protection

OFFICIAL USE ONLY

potential injury to the United States.¹⁵ The defendant in a criminal proceeding must likewise have access to it, since the information itself may tend to exculpate him with respect to dealings in it.¹⁶ As Judge Learned Hand said in *U.S. v. Andolschek*, "The Government must choose; either it must leave the transactions in the obscurity from which a trial will draw them, or it must expose them fully."¹⁷

These rulings have left the government in the position of having to reveal in court the very information it is trying to keep secret or else not prosecute those who steal information and use it to the injury of the nation. To invoke the law's protection of the secret, the secret must be told.

Judicial experience with the privilege which protects military and state secrets has been limited in this country.¹⁸ British experience, though more extensive, is still slight compared to that with other evidentiary privileges.¹⁹ Nevertheless, it is clear at least from the civil precedents that the court itself must determine whether the circumstances are appropriate for the claim of privilege²⁰ and yet do so without forcing a disclosure of the very thing the privilege is designed to protect.²¹ The latter requirement is the real difficulty. In dealing with it, courts have found it helpful to draw upon judicial experience

¹⁵ *Gorin v. U.S.*, 312 U.S. 19, 30-31, *supra* note 14.

¹⁶ *U.S. v. Reynolds*, 345 U.S. 1, 73 S.Ct. 538 (1953); *Jencks v. U.S.*, *supra* note 7.

¹⁷ 142 F.2d 503, 506 (1944).

¹⁸ See *Totten v. U.S.*, 93 U.S. 105, 23 L.Ed. 605 (1876); *Firth Sterling Steel Co. v. Bethlehem Steel Co.*, 199 Fed. 353 (1912); *Pollen v. Ford Instrument Co.*, 28 F. Supp. 583 (1939); *Cresmer v. U.S.*, 9 F.R.D. 203 (1949). See also *Bank Line v. U.S.*, 68 F. Supp. 587, 163 F.2d 133 (1947). 8 Wigmore on Evidence (3d Ed.) sec. 2212(a), p. 161, and sec. 2378(g)(5), pp. 785 et seq.; 1 Greenleaf on Evidence (16th Ed.) secs. 250-251; Sanford, Evidentiary Privileges Against the Production of Data Within the Control of Executive Departments, 3 Vanderbilt Law Review 73-75 (1949). See also *Ticon v. Emerson*, 134 N.Y.S. 2d 716, 206 Misc. 727 (1954).

¹⁹ Most of the English precedents are reviewed in *Duncan v. Cammel, Laird & Co., Ltd.*, A.C. 624 (1942). For a thorough study of the history and application of the Official Secrets Acts see David Williams' *Not in the Public Interest* (London, 1965), reviewed in *Studies* X 3, p. 97.

²⁰ *Id.* at 842.

²¹ *U.S. v. Reynolds*, *supra* note 16, at 8, citing *Duncan v. Cammel, Laird & Co., Ltd.*, *supra* note 19, and *Hoffman v. U.S.*, 341 U.S. 478 (1951).

OFFICIAL USE ONLY

75

OFFICIAL USE ONLY

Legal Protection

in dealing with an analogous privilege, that against self-incrimination. The Supreme Court said in *U.S. v. Reynolds*:²²

The privilege against self-incrimination presented the courts with a similar sort of problem. Too much judicial inquiry into the claim of privilege would force disclosure of the thing the privilege was meant to protect, while a complete abandonment of judicial control would lead to intolerable abuses. Indeed, in the earlier stages of judicial experience with the problem, both extremes were advocated, some saying that the bare assertion by the witness must be taken as conclusive, and others saying that the witness should be required to reveal the matter behind his claim of privilege to the judge for verification. Neither extreme prevailed, and a sound formula of compromise was developed. . . .

Regardless of how it is articulated, some like formula of compromise must be applied here. Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers. Yet we will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case. It may be possible to satisfy the court, from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the occasion for the privilege is appropriate, and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.²³

Of course *Reynolds* was a civil case, but the evidentiary difficulty in criminal cases is quite comparable. Thus, citing *Reynolds*, the Supreme Court stated in *Jencks v. U.S.*:²⁴

It is unquestionably true that the protection of vital national interests may militate against public disclosure of documents in the Government's possession. This has been recognized in decisions of this Court in civil causes where the Court has considered the statutory authority conferred upon the departments of government to adopt regulations not inconsistent with law for . . . use . . . of the records, papers, appertaining to his department. The Attorney General has adopted regulations pursuant to this authority declaring all Justice De-

²² *Supra* note 16, at 8-10.

²³ In *Kaiser Aluminum & Chemical Corp. v. U.S.*, 157 F. Supp. 939 (1958), the Court of Claims held that judicial examination of a document for which executive privilege has been asserted should not be ordered without a definite showing by plaintiff of facts indicating reasonable cause for requiring such a submission. Otherwise, said the Court, at 949, the executive determination would be merely preliminary and "the officer and agency most aware of the needs of government and most cognizant with [sic] the circumstances surrounding the legal claim will have to yield determination to another officer (the Court) less well equipped."

²⁴ *Supra* note 7, at 670.

Legal Protection

OFFICIAL USE ONLY

partment records confidential and that no disclosure, including disclosure in response to subpoena, may be made without his permission.

But this Court has noticed, in *U.S. v. Reynolds*, the holdings of the Court of Appeals for Second Circuit that, in criminal causes "... the Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense. ..."

The loophole afforded by this evidentiary difficulty has not been overlooked by the thief who limits his trade to information too sensitive to be revealed. Nor is it ignored by the more imaginative among those accused of other crimes when they claim that their offenses were committed at the behest of an intelligence agency which uses its statutory shield to protect itself at the expense of its agent.

Judicial Evaluation of Sensitive Data

It must be emphasized that undesired disclosure is only one difficulty in the submission of intelligence data to a jury. There is another great problem, the capability of the jury to evaluate such data, often complex and technical and often meaningful only in the context of other sensitive information not otherwise bearing on the case.²⁶ It can of course be argued that juries often have to grapple with technical facts and that the law provides for assistance in such instances in the form of expert witnesses. But in a case dealing with secret information, resort to these legal devices merely increases the amount of sensitive data which must be shorn of its usefulness by disclosure, increasing the government's reluctance to prosecute and thwarting the protective congressional intent expressed in legislation.

Some Avenues for Action

The courts have recognized that intelligence activities are confidential *per se* and not subject to judicial inquiry. Congress, in the National Security Act, has charged the Director of Central Intelligence with the protection of intelligence sources and methods and has given

²⁶ The quoted material from the *Reynolds* case appears at 345 U.S. 12.

²⁷ Compare the holding in the *Kaiser* case, *supra* note 23, on the competence of the court to evaluate the contents of a document for which there has been a claim of executive privilege.

OFFICIAL USE ONLY

Legal Protection

him certain statutory authority and exemptions to assist him in meeting this obligation. Yet the espionage laws and related statutes enacted for the same or a similar purpose can often not be put to work just when the offense represents the greatest potential threat to the public welfare.

There are three steps which would go far toward solving the problems which still exist in this area. Two of them would seem to require new legislation; the third might be accomplished, at least with respect to CIA, by regulation under the DCI's existing authority. First would be a criminal statute defining what is to be protected and providing punishment for exposure. Second, this statute should also confer injunctive authority, because prevention of exposure is more to the point than punishment for violation and in many cases an injunction might offer greater deterrence than the penal provisions for violation. In addition, the act might provide that persons convicted under it would forfeit retirement benefits; precedent for this exists in 5 U.S.C. §8312, the so-called "Hiss Act."

The third step would be a requirement by the Director that all employees, agents, consultants, and others who enter into a relationship with CIA giving them privity to intelligence data agree in writing to assign as of that time to the Agency all rights in anything intended by them for publication based on information received in the course of their official duties. Perhaps a similar step could be taken by other intelligence agencies. Such agreements, along with appropriate regulations governing the dissemination of intelligence data, could in themselves serve as a basis for injunctive relief, apart from or as an alternative to the statutory provision for injunctions against the criminal act of exposure.

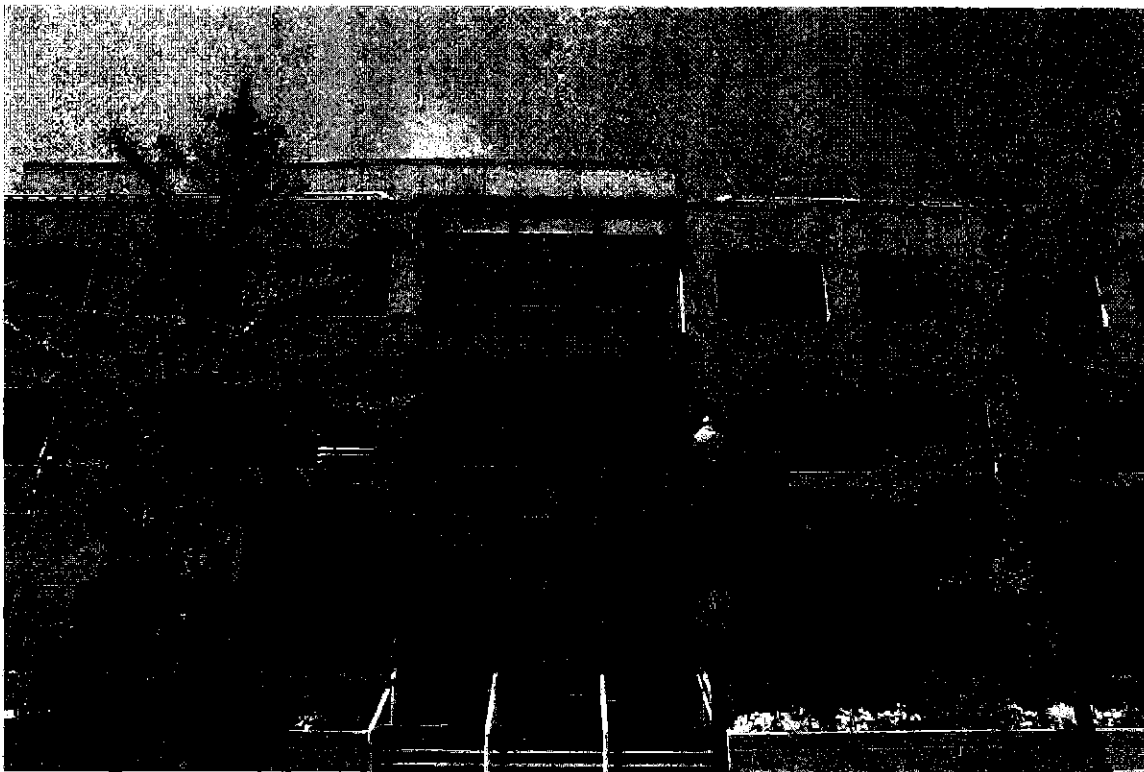
Some such steps are necessary if we are to overcome the shortcomings in laws protecting intelligence information which limit prosecution to cases where intent is clear and where divulging information in open court is not detrimental.

Tab D

The Atlantic

Did Putin Direct Russian Hacking? And Other Big Questions

Did Moscow influence the U.S. election? Who else has been hacked?
Could the CIA be wrong?



Gary Cameron / Reuters

KATHY GILSINAN AND KRISHNADEV CALAMUR

JAN 6, 2017 | GLOBAL

Like *The Atlantic*? Subscribe to The Atlantic Daily, our free weekday email newsletter.

Email

SIGN UP

Updated on January 7, 2017

In a “declassified version of a highly classified assessment” released on Friday January 6, the U.S. intelligence community laid out its judgment that “Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election,” with the specific goal of harming Hillary Clinton’s “electability and potential presidency.” The report went on: “We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.”

These conclusions had previously been reported, based accounts anonymous intelligence officials gave to various news outlets. The January 6 intelligence assessment was the first time the Office of the Director of National Intelligence had detailed them officially in public.

The release came a day after Senator John McCain, the Arizona Republican who chairs the Senate Armed Services Committee, said at a hearing on foreign cyberthreats to the United States: “Every American should be alarmed by Russia’s attacks on our nation.” (Our blog of the hearing is [here](#).)

President-elect Donald Trump has been publicly skeptical of claims about Russia’s role. He says it’s difficult to definitively say who was behind the hacking, and has supported the views of Julian Assange, the WikiLeaks founder, that a “14-year-old could have hacked” Democratic officials. After reviewing a classified version of the assessment made public on Friday, Trump issued a statement citing the cyber threat from “Russia, China, other countries, outside groups and people,” but emphasizing that the hacking had “absolutely no effect on the outcome of the election.”

Last month McCain told Ukrainian TV Russia's actions were "an act of war." He repeated those comments Thursday, but added: It "doesn't mean you go to war and start shooting."

Who is involved?

The intelligence-community assessment provides official backing to media reports from mid-December stating that that Russian President Vladimir Putin was "personally involved" in cyberattacks aimed at interfering with the United States presidential election. In an interview with NPR on December 15, U.S. President Barack Obama vowed that the U.S. would take action in response, "at a time and place of our own choosing." He went on: "Mr. Putin is well aware of my feelings about this, because I spoke to him directly about it." On December 29, he did more than speak: He sanctioned the two Russian intelligence services believed to be involved in the hacks (Russian military intelligence, the GRU, and the KGB's successor the FSB, which is responsible for counterintelligence and internal security). He also expelled 35 Russian officials in the U.S. believed to be intelligence agents. After Russian Foreign Minister Sergei Lavrov threatened to retaliate, Putin declined to do so.

Didn't we already know about Russia hacking the Democratic National Committee and others? Why all the fuss?

The assessment purports to add on-the-record detail on both actors and intent. Prior to mid-December, Putin personally had not been blamed for hacks resulting in leaks damaging to the Clinton campaign, though in October Director of National Intelligence James Clapper stopped just short of doing so, saying that "based on the scope and sensitivity of these efforts ... only Russia's senior-most officials could have authorized these activities." Secondly, separate intelligence leaks to *The New York Times*

and *The Washington Post* on December 9 for the first time claimed that the intent of the hacking was to sway the election in favor of Trump, rather than simply sow generalized distrust. It has not yet been suggested that cyberattacks managed to change the actual vote tally in favor of either presidential candidate. This is now the official position of the intelligence community.

Information on what exactly happened has been dripping out slowly, and often anonymously and unofficially, for months. Way back in mid-June, the Democratic National Committee reported an intrusion into its computer network, and the cybersecurity firm CrowdStrike publicly blamed Russian hackers after analyzing the breach. In July, after emails stolen from the committee appeared on WikiLeaks, Democratic members of congress also blamed the Russians, with Clinton campaign manager Robby Mook alleging that “It was the Russians who perpetrated this leak for the purpose of helping Donald Trump and hurting Hillary Clinton.”

It wasn’t until September that anonymous federal officials confirmed to *The New York Times* the intelligence community’s “high confidence” of Russian government involvement in the hack, if not the subsequent leak, and leaving doubt as to whether the hacks were “routine cyberespionage” or actually intended to influence the election. And it wasn’t until October that the Director of National Intelligence, James Clapper, went on the record to blame Russia—government actors, not, say, cybercriminals who happened to be Russian, “based on the scope and sensitivity of these efforts,” and further declaring that they were “intended to interfere with the U.S. election process.” Days later, emails stolen from Clinton campaign chairman John Podesta appeared on WikiLeaks.

So as of fall, the United States government had officially blamed Russia for the hacks, and stated that the hacks were intended to interfere with the

American election. Until December 9, intelligence officials were not claiming that the Russians wanted specifically to help Trump win, as opposed to undermining faith in the overall process. Then *The Washington Post* disclosed a “secret CIA assessment”—again described by anonymous officials—declaring it “quite clear” that a Trump presidency was the ultimate goal of the hacks. A *Times* investigation published a few days later provided more background on how the hacks actually worked. Congress is planning to investigate.

Who else has been hacked?

Thomas Rid, writing in *Esquire* in October, noted that Russia began hacking the U.S. as early as 1996, five years after the demise of the Soviet Union, and added that the DNC hack concealed an even bigger prize for the Russians: the National Security Agency, whose secret files were dumped this August on Github and other file-sharing sites.

Then there is Germany. In May, BfV, Germany’s domestic intelligence agency, said hackers linked to the Russian government had targeted Chancellor Angela Merkel’s Christian Democratic Union party, as well as German state computers. In September, Arne Schoenbohm, who heads Germany’s Federal Office for Information Security (BSI), briefed German lawmakers about Russian hacking. Schoenbohm told *Süddeutsche Zeitung*, after reports emerged in the U.S. of the hacking of the Democratic National Committee, that “[g]iven the background of the American situation, I have to protect our political parties from spying.” Those warnings became more urgent after the U.S. presidential election. Bruno Kahl, the head of the Germany’s foreign intelligence service, told the newspaper last month that Russia could seek to disrupt Germany’s elections next year to create “political uncertainty.” Merkel, who is seeking a fourth term in those elections, said in November after an attack

targeted Deutsche Telekom customers that “[s]uch cyber attacks, or hybrid conflicts as they are known in Russian doctrine, are now part of daily life and we must learn to cope with them.”

Suspected Russian hacking has targeted other countries, as well. In April 2007, websites and servers belonging to the government, banks, and media in the former Soviet republic of Estonia came under a sustained monthlong attack. A U.S. diplomatic cable, published in WikiLeaks, called the Baltic state an “unprecedented victim of the world's first cyber attacks against a nation state.” Similar attacks targeted the former Soviet republic of Georgia a year later, and Ukraine more recently. All three countries have pro-Western leaders that are deeply critical of what they see as Russia’s turn toward authoritarianism under President Vladimir Putin.

And prior to perhaps their most high-value target thus far, the DNC, Russian hackers allegedly targeted the World Anti-Doping Agency ahead of the Rio Olympics this summer. WADA had reported a widespread Russian state-run doping program that involved the country’s track-and-field program. That revelation resulted in the Russian track-and-field team being banned from the games. WADA was hacked in apparent response, and the personal information of several athletes, including the Russian whistleblower who alerted WADA to the scandal, was leaked online. It’s worth pointing out that the Russian government has dismissed claims that it is involved.

What does “hacking” actually entail?

It depends: Hackers believed to be from Russia have accessed computers and servers belonging to government and political parties in rival countries. In some cases, such as in the DNC or WADA hack, those hacks resulted in the leak of information on websites such as WikiLeaks. In other

cases, the attacks focused on national infrastructure: In Ukraine, for instance, according to *Wired*, hackers targeted the power grid; they then attacked the telephone service so customers couldn't call to report the outages. When they hit the NSA, hackers posted the agency's "cyber-weapons" to file-sharing sites, according to *Esquire*. The hackers don't just target states and institutions. Frequently, individuals are caught up, as well. On December 9, the *Times* reported that suspected Russian hackers targeted critics of the country's government who live overseas by posting child porn on their computers.

How solid is the intelligence community's case that Russia tried to tilt the election for Trump?

The *Washington Post* has cited "the United States' long-standing struggle to collect reliable intelligence on President Vladimir Putin and those closest to him." Since the end of the Cold War and especially since 9/11, American intelligence agencies have deprioritized Russia. The *Post* reported in fall, citing U.S. officials, that the "CIA and other agencies now devote at most 10 percent of their budgets to Russia-related espionage, a percentage that has risen over the past two years," but is still dwarfed by the Cold War peak of about 40 percent.

As for the actual evidence of intent, what's publicly available remains circumstantial, including Russian state TV's pushing of Trump's candidacy, and reports that the Republican National Committee, too, was hacked though suffered none of the same embarrassing leaks as the DNC. (The RNC has denied it was hacked; *The Wall Street Journal* reports, citing "officials who have been briefed on the attempted intrusion," that the effort was thwarted by the RNC's cybersecurity systems.) All of this was occurring in an international political context in which Trump was one of the most pro-Russian presidential candidates in recent memory, while

Vladimir Putin personally blamed Hillary Clinton for inciting protests against his rule when she was secretary of state.

In tandem with Obama's announcement of sanctions against Russia on December 29, the Department of Homeland Security and the FBI released a joint report on "Russian malicious cyber activity" during the U.S. election. That report, however, was short on specific evidence; moreover, *The New York Times* noted, it "included a long list of malware it said was evidence of Russian hacking, when some of the malware is used by non-Russian attackers."

Meanwhile, the denials. Some of Trump's surrogates have publicly suggested that Russia is the victim of a false-flag operation planned by U.S. intelligence—an assertion that doesn't appear to be based on any fact in the public realm. Russian officials themselves have rejected the idea they are involved, as have Russian cybersecurity experts, one of whom dismissed it as "a classic stereotype of the nineties and early 2000s." They say that it's virtually impossible to trace the origin of a hack. For his part, the president-elect tweeted the claim of WikiLeaks founder Julian Assange that, in Trump's words, "the Russians did not give him the info!" and that "a 14 year old could have hacked Podesta."

As Kaveh Waddell explained in *The Atlantic*, while it can be difficult to catch the culprit of a hack, it's by no means impossible. *Esquire*, in its story, noted that sloppy errors committed by the hackers pointed U.S. intelligence to their whereabouts. Andrei Soldatov, who wrote *Red Web*, told *The Telegraph* the Russian government is using its computer industry to hack its targets. "We have maybe the biggest engineer community in the world, and lots of great specialists," he told the newspaper. "They are not criminals, they are professionals—and they are not bothered or afraid to refuse requests from government agencies."

But Trump says we shouldn't trust the CIA because they were wrong about Iraq's WMD. Shouldn't we take that history into consideration?

"There's a big difference between Iraq WMD and Russian cyber hacking," wrote Amy Zegart, an intelligence expert at Stanford, in an email. "For starters, we're talking about different people making the assessments, a different problem to unravel (hidden nuclear capabilities in a foreign country versus cyber attacks on US systems), and a different analysis process. Intelligence analysis was thoroughly revamped after Iraq, as it should have been. But saying that these are same people who brought us Iraq WMD is like saying this year's Golden State Warriors must be terrible, because the Warriors lost so many games in the 90s."

Which isn't to say that past intelligence failures writ large have no relevance to today. The relevance is: Intelligence sometimes fails. As Zegart notes: "The best experts didn't predict Trump's win, and that's Americans predicting what Americans will do in an open society with frequent polling. In intelligence, adversaries are working hard and spending billions to hide their activities and deceive us."

Kenneth Pollack, a former CIA analyst and Clinton National Security Council staffer who argued for invading Iraq in 2003, said in an interview that Saddam Hussein did a "totally insane" version of this: "Saddam's whole thinking was, 'I'm going to get rid of my weapons of mass destruction, basically after 1995, but I can't tell my people that. I want my people to continue to fear me, and believe that I have this.' ... The U.S., and the rest of the world, frankly ... all picks up on the fact that that he is putting it out to all of his people that, 'Yeah I still have WMD.' And that strikes me as a really fundamental difference."

He continued: “The intelligence community certainly can be wrong about these kinds of things, and you do want to take everything with a certain amount of skepticism. That said, it seems like in this case, they’ve found the tracks—that’s kind of the nice thing about cyber, as best as I understand it, is you can actually go back and see the keystrokes ... which was not something that we had in Iraq.”

Do you have any lingering questions about Russian hacking? Please let us know and we’ll try to answer them: hello@theatlantic.com.

ABOUT THE AUTHORS



KATHY GILSINAN is a senior editor at *The Atlantic*, where she oversees the Global section.

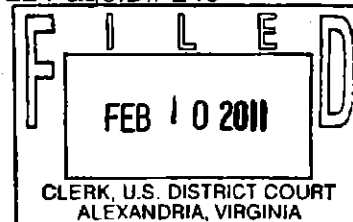
Twitter Email



KRISHNADEV CALAMUR is a senior editor at *The Atlantic*, where he oversees news coverage. He is a former editor and reporter at NPR and the author of *Murder in Mumbai*.

Twitter

Tab E



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	
	)	NO. 1:10CR485 (LMB)
JEFFREY ALEXANDER STERLING,	)	
	)	
Defendant.	)	
	)	
	)	

PROTECTIVE ORDER REGARDING CLASSIFIED INFORMATION

This matter had come before the Court upon the *Motion for Protective Order Under Section 3 of the Classified Information Procedures Act* to prevent the unauthorized disclosure or dissemination of classified national security information and documents which will be reviewed or made available to the defendant and his counsel by the government during the prosecution of this case. Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. 3 (2006) ("CIPA"), the Security Procedures Established Pursuant to CIPA by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA section 9), Rules 16(d) and 57 of the Federal Rules of Criminal Procedure, and the general supervisory authority of the Court, and in order to protect the national security, the following Protective Order is entered:

I. The Court finds that this case will involve information that has been classified in the interest of the national security. The storage, handling and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to which requires the appropriate security clearances. The purpose of this Order is to

5. In accordance with the provisions of CIPA and the security procedures promulgated by the Chief Justice of the United States pursuant to that Act, this Court designates Christine Gunning as the Classified Information Security Officer and Jennifer Campbell, Winfield Slade, Maura Peterson, and Joan Kennedy as alternate Classified Information Security Officers for this case for the purpose of providing security arrangements necessary to protect any classified information or documents that will be made available to the defense in connection with this case or that may be in the possession of the defense as a result of the defendant's prior relationship with the government. Defense counsel shall seek guidance from the Classified Information Security Officer with regard to appropriate storage, handling, transmittal, and use of all classified information.

6. The Court has been advised that the Department of Justice Attorneys assigned to this case, William M. Welch II, Timothy J. Kelly, and James L. Trump, as well as Legal Administrative Specialist Gerard Francisco and Intelligence Specialist Pam Benson, have the requisite security clearances allowing them to have access to the classified documents and information that relate to this case (hereinafter "government attorneys"). Any references to government attorneys as used in this Order refer only to the attorneys listed in this paragraph. Any other Department of Justice attorneys who may in the future be designated to participate in the litigation of any part of this matter (or supervise such litigation) will have security clearances at the level of classification of any documents or information reviewed.

7. The defendant's counsel, Edward B. MacMahon, Jr., James H. Holt, and Barry J. Pollack, shall be given access to classified national security documents and information as required by the government's discovery obligations and in accordance with the terms of this

Protective Order, the requirements of CIPA, the Memorandum of Understanding described below, and any other orders issued pursuant to CIPA, and upon receipt of appropriate security clearances. Defendant Jeffrey Alexander Sterling (hereinafter "the defendant") will also be given access to national security documents and information as required by government discovery obligations and in accordance with the terms of this Protective Order, the requirements of CIPA, the Memorandum of Understanding described below, and any other orders issued pursuant to CIPA. To date, defense counsel and the defendant will be given access to the same classified information except that the defendant will not be granted access to the technical documents underlying Classified Program No. 1 at this time.

8. As set forth in the Government's Motion for Protective Order, the defendant has a continuing contractual obligation to the government not to disclose to any unauthorized person classified information known to him or in his possession. The government is entitled to enforce its agreement to maintain the confidentiality of classified information. Notwithstanding that agreement, because the allegations of this case involve a breach of that non-disclosure obligation, the defendant must sign a separate Memorandum of Understanding. Consequently, pursuant to federal common law, the ordinary principles of contract law, and the contempt powers of this Court, the defendant shall fully comply with his nondisclosure agreements and shall not disclose any classified information to any unauthorized person unless authorized to do so by this Court. reviewed.

9. Any additional persons whose assistance the defense reasonably requires may only have access to classified information in this case after first obtaining from this Court, with prior notice of the identity of those additional persons to the government attorneys, an approval

assisting the defense, to have access to classified information.

Entered in Alexandria, Virginia, this 10th day of February, 2011.



Leonie M. Brinkema
United States District Judge

CERTIFICATE OF SERVICE

I hereby certify that I have this day served a copy of the foregoing **DEFENDANT'S MOTION AND BRIEF IN OPPOSITION TO THE GOVERNMENT'S MOTION FOR A PROTECTIVE ORDER**, by using the CM/ECF system which will automatically send notification of such filing to the following:

James D. Durham, Esquire
Acting US Attorney
Jennifer G. Solari, Esquire
Assistant US Attorney
Southern District of Georgia
PO Box 8970
Savannah, GA 31401

Julie A. Edelstein, Esquire
David C. Aaron, Esquire
US Department of Justice
National Security Division

This 20th day of July, 2017

s/ John C. Bell, Jr.
John C. Bell, Jr.

COUNSEL FOR DEFENDANT